AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Previously Presented) In a computer-implemented authorization management system, a method for controlling a user's access to a computing resource that is managed by said computer-implemented authorization management system, the method including:

receiving an electronic request for the computing resource;

retrieving a group of computer-readable authorization certificates from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system, each certificate containing at least one computer-readable authorization by at least one principal;

identifying a set of principals associated with the group of computer-readable authorization certificates;

creating a lattice of authorization values associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system, wherein the lattice of authorization values is a monotone function of one or more authorization values of the set of principals;

evaluating a certificate as a monotone function, at least in part, of the one or more authorization values associated with one or more of the principals;

updating the one or more authorization values of one or more of the principals if the result of said evaluating step indicates that an authorization value of a principal

should be changed, the step of updating the authorization value being a monotone function; and

repeating said evaluating and updating steps until a steady state of said lattice of authorizations values is reached.

2. (Previously Presented) A method as in claim 1, further including:

constructing a dependency graph representation in a memory device in communication with the computer-implemented authorization system, the dependency graph containing a node corresponding to each principal in the set of principals; and

assigning at least two nodes in the dependency graph with a certificate that expresses a dependency of one node on the state of another node;

wherein the dependency graph representation is used, at least in part, during said evaluating, updating, and repeating to determine which certificates to evaluate.

3. (Previously Presented) A method as in claim 1, in which said updating is performed after all of the certificates have been evaluated.

4. (Previously Presented) A method as in claim 1, in which the request for the computing resource is received from a first principal, and in which at least one of the certificates is received from the first principal, the certificate having been issued by a second principal.

5. (Original) A method as in claim 1, in which the certificates comprise Simple Public Key Infrastructure certificates.

6. (Previously Presented) A method as in claim 1, in which the electronic request is to access to a piece of electronic content; use a computer program; execute a transaction; access a computer; or access a network.

7. (Currently amended) A computer program product for making authorization management determinations for controlling a user's access to a computing resource that is managed by said computer-implemented authorization management system, the computer program product including the ~~step~~steps of:

receiving an electronic request to perform a predefined action;

retrieving a group of computer-readable authorizations for the predefined action from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system, one or more of the computer-readable authorizations in the group being a monotone function of the authorization state of one or more principals;

identifying a set of principals associated with the group of computer-readable authorizations and for initializing a lattice of authorization values associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system;

evaluating one or more authorizations in the group of computer-readable authorizations using an authorization value associated with each principal;

updating the authorization value of one or more principals in the set of principals, the updating of the authorization ~~valve~~ value being a monotone function;

causing repeated execution of said computer code for evaluating one or more authorizations in the group of computer-readable ~~authorization~~ authorizations and for updating the authorization value of one or more principals in the set of principals until a steady state of said lattice of authorization values is reached; and

storing the computer codes.

8. (Previously Presented ) A computer program product as in claim 7, in which the computer-readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, network server, hard drive, and optical storage.

9. (Previously Presented) A computer-implemented system for controlling access to electronic content or processing resources managed by a computer-implemented authorization management system, the system comprising:

means for receiving an electronic request from a requesting principal to access a piece of electronic content or a processing resource;

means for collecting a set of one or more computer-readable authorization certificates relating to the request, the requesting principal, or the piece of electronic content or processing resource from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system;

means for identifying a root principal from whom authorization is needed in order to grant the electronic request;

means for creating a lattice of monotone authorization values in a memory device associated with a memory device in communication with said system and performing at least a portion of a least fixpoint computation over said authorization values to determine whether the root principal has authorized the requesting principal to access the piece of electronic content or processing resource; and

means for granting the requesting principal access to the piece of electronic content or processing resource when the least fixpoint computation indicates that the root principal has authorized said access.

10. (Previously Presented) A computer-implemented system for controlling access to electronic resources, the system comprising:

a first computer system for processing electronic requests for access to electronic resources, the first computer system comprising:

a computer network interface configured to receive digital certificates from other computer systems and for electronically receiving and processing requests to access electronic resources;

a memory device in communication with said first computer system for storing electronic resources and one or more computer-readable authorization certificates relating to authorization for controlling access thereto; and

a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by creating a

lattice of monotone authorization values in a memory device associated with a memory device in communication with said system and performing least fixpoint computations using said authorization values.

11. (Previously Presented) A system as in claim 10, further comprising:

a second computer system for making a request for electronic resources from the first computer system; and

a third computer system for generating a first digital certificate, the first digital certificate including an authorization value that is generated from a first monotone function, the authorization value effective for authorizing, at least in part, the second computer system to access a predefined electronic resource.

12. (Previously Presented) A system as in claim 11, further comprising:

a fourth computer system, the fourth computer system being operable to generate a second digital certificate including an authorization value that is generated from a second monotone function, the second digital certificate authorizing, at least in part, the third computer system to authorize, at least in part, the user of the second computer system to access the predefined system resource.

13. (Previously Presented) A system as in claim 12, in which the third computer system is operable to transmit the first digital certificate to the second computer system, the second computer system is operable to transmit the first digital certificate to the first

computer system in connection with said request, and the fourth computer system is operable to transmit the second digital certificate to the first computer system.

14. (Previously Presented) A system as in claim 13, in which the first computer system further comprises a public key stored in a memory device in communication with said first computer system and associated with the fourth computer system, the public key corresponding to a private key used to sign the second digital certificate.

15. (Original) A system as in claim 10, in which at least some of the digital certificates comprise SPKI certificates.

16. (Original) A system as in claim 10, in which at least some of the digital certificates comprise Keynote certificates.

17.–20. (Cancele )